IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DAV SUB, INC. (d/b/a CONTINUUM HEALTH TECHNOLOGIES CORP.), **Plaintiff,** **v.** **QLIQSOFT, INC.,** **Defendant.**	**CIVIL ACTION NO.: 3:23-cv-02504** **JURY TRIAL DEMANDED**

PLAINTIFF'S FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

1. Plaintiff DAV Sub, Inc. (d/b/a Continuum Health Technologies Corp.) ("Continuum" or "Plaintiff") files this first amended complaint ("FAC") against QliqSOFT, Inc. ("QS" or "Defendant") as a matter of right pursuant to Federal Rule of Civil Procedure 15(a)(1)(B).

2. This is an action under the patent laws of the United States, Title 35 of the United States Code (35 U.S.C. §§ 271, 286), for patent infringement in which Plaintiff makes the following allegations against Defendant.

PARTIES

3. Plaintiff is a Delaware company, having its primary office at 801 Barton Springs Rd., Floor 9, Austin, TX 78704.

4. Defendant is a Delaware company with its principal place of business at 13155 Noel Rd., Suite 900, Dallas, TX 75240, and has already made an appearance in this case.

JURISDICTION AND VENUE

5. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

6. Venue is proper in this district under 28 U.S.C. §§ 1391(c), generally, and under 1400(b), specifically. Defendant has a regular and established place of business in this Judicial District, and Defendant has also committed acts of patent infringement in this Judicial District.

7. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

8. Defendant has established offices in Dallas, Texas – within the Northern District of Texas.

9. Defendant has infringed, and does infringe, by transacting and conducting business within the Northern District of Texas. Upon information and belief, operations at Defendant's Dallas location include sales, marketing, business development, and/or technology development for Defendant's infringing instrumentalities.

10. Defendant's office in Dallas, Texas is a regular and established place of business in this Judicial District, and Defendant has committed acts of infringement (as described in detail, hereinafter) at Defendant's office within this District. Venue is therefore proper in this District under 28 U.S.C. § 1400(b).

FACTUAL BACKGROUND – PLAINTIFF'S PATENTS

11. Plaintiff is a software company providing healthcare related software as a service ("SaaS") products and systems ("Plaintiff's Systems"). The development of the Plaintiff's core intellectual property began in the early 2000's and has continued ever since.

12. Plaintiff currently owns a half dozen issued U.S. Patents, reading upon various healthcare related technologies and operations - including, but not limited to: healthcare related revenue cycle management; HIPAA secure messaging; telehealth operations; healthcare payment systems; secure file sharing; and mobile applications and interfaces for a variety of users and resource providers.

13. Plaintiff currently owns multiple pending U.S. Patent applications, directed to its healthcare related technologies and operations, in addition to innovative technologies and systems.

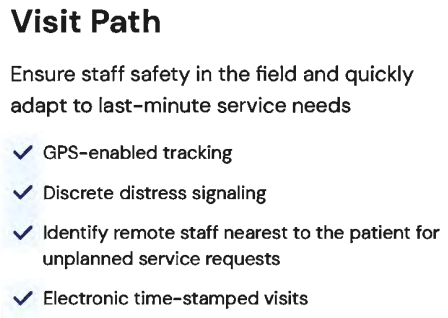
14. Plaintiff has invested, and continues to invest, substantial resources – both in terms of time and costs – to procure and develop patents that protect its intellectual property.

15. Plaintiff's Systems implement and practice the inventions disclosed and claimed in the U.S. Patents owned by Plaintiff.

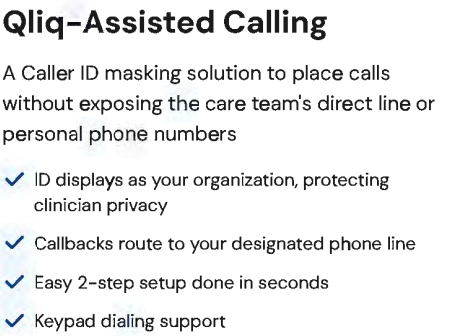
DEFENDANT'S INFRINGING INSTRUMENTALITIES

16. Defendant directly – or through intermediaries including distributors, partners, contractors, employees, divisions, branches, subsidiaries, or parents – made, had made, used, operated, imported, provided, supplied, distributed, offered for sale, sold, and/or provided access to software systems, cloud-based software, and/or smart device apps for peer-to-peer messaging between healthcare professionals, ancillary service providers, administrative staff, caregivers, or patients – including, but not limited to, Defendant's QliqCHAT systems and platforms ("QliqCHAT Platform").

17. Defendant's publicly available information indicates that add-ons to the QliqCHAT include: Visit Path,

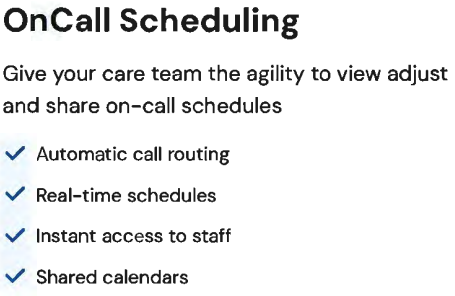


Qliq-Assisted Calling,



Snap & Sign,

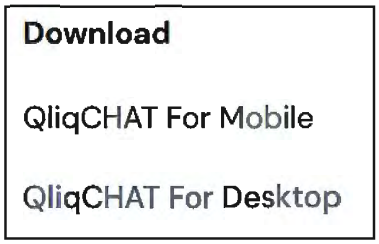
OnCall Scheduling,



and QliqSTOR (collectively, the "QliqCHAT Add-Ons").

The QliqCHAT Platform operating in conjunction with the QliqCHAT Add-Ons (collectively, "QS Software Systems") are the infringing instrumentality(ies).

18. Defendant's publicly available information indicates that the infringing instrumentalities operate using mobile and desktop computing and communications devices, and computer server and storage systems.



19. Defendant's publicly available information indicates that the infringing instrumentalities comprise a messaging service, wherein everything is cloud based except the message archival server, QliqSTOR.

20. Defendant's publicly available information indicates that the infringing instrumentalities utilize an individual public/private key encryption model.

21. Defendant's publicly available information indicates that the infringing instrumentalities encrypt/decrypt all messages on a user's mobile device(s) and computers, where they are stored in an encrypted database.

22. Defendant's publicly available information indicates that the infringing instrumentalities provide: GPS-enabled tracking, discrete distress signaling, identify remote staff nearest to the patient for unplanned service requests, electronic time-stamped visits, customizable message notification and sound alerts; message delivery confirmation; manual message acknowledgment; custom lists of quick messages; the ability to send images/videos/files/voice messages; organization of users by groups/subgroups; inclusion of external users; centralized administration; remote lock and wipe; message archiving; and EHR and directory integration.

23. Defendant's publicly available information indicates that the infringing instrumentalities operate such that the mobile application is always on, whether in the foreground or the background.

24. Defendant's publicly available information indicates that the infringing instrumentalities operate such that a mobile number is not required to route messages - real-time communication can occur from a desktop, smartphone, or tablet.

25. Defendant's publicly available information indicates that the infringing instrumentalities directly integrate with EHRs and other clinical systems through the interface engine QliqSTOR, which uses HL7 2.x standards and above to interconnect with the QS Software Systems.

26. Defendant's publicly available information indicates that the infringing instrumentalities send non-secure notifications to non-secure devices.

27. Defendant's publicly available information indicates that the infringing instrumentalities utilize a distributive architecture where data is stored on a customer's devices and servers.

28. Defendant's publicly available information indicates that the infringing instrumentalities use a cloud-based SIP server for real-time message routing and delivery. All messages are end-to-end encrypted so only the sender can encrypt the message and the intended recipient can decrypt the message.

29. Defendant's publicly available information indicates that the infringing instrumentalities comprise a peer-to-peer architecture that uses a combination of Public and Private Keys. All messages are deleted from QS Software Systems servers immediately upon delivery - encrypted messages are transiently stored on the servers if a recipient is offline.

30. Defendant's publicly available information indicates that the infringing instrumentalities operate such that a sender can initiate messages even if a network connection is unavailable. The messages are automatically delivered when the sender goes online.

31. Defendant's publicly available information indicates that the infringing instrumentalities operate such that they will automatically lock after a pre-defined amount of inactivity or idle time. Both end-users and administrators can remotely lock and wipe the application data by logging into an administrative dashboard on Defendant's website.

32. Defendant's publicly available information indicates that the infringing instrumentalities operate such that messages are stored locally in an encrypted database on a user's smartphone, tablet, or desktop, but are automatically deleted according to the message expiration set by an administrator. A user has the option to delete messages and attachments sooner if desired.

33. Defendant's publicly available information indicates that the infringing instrumentalities operate such that by default, messages will expire and be deleted from the end-user QliqCHAT application, depending upon the user. For some users, messages automatically

expire after 7 days. Administrators can select the message retention rate. Messages can be archived for a longer period by the organization using the QliqSTOR archive.

34. Defendant's publicly available information indicates that the infringing instrumentalities operate such that policies are administered through the Defendant's Business/Enterprise web console under the direction of an administrator.

35. Defendant's publicly available information indicates that the infringing instrumentalities operate such that all messages and their status are individually date/time stamped. If an intended recipient is offline, the status shows "Offline." When the recipient receives the message, the status on the sender's device changes to "Delivered" and when the message is viewed the status changes to "Read." In addition to message logging, the infringing instrumentalities allow senders to request an acknowledgment from the receiver. This functionality ensures that messages are received, read, and understood. The acknowledgment itself is also date/time stamped. By touching or right clicking a mouse over a message segment, an option appears to view message details, which include message id, the date/time it was created, sent, received, and read.

36. Defendant's publicly available information indicates that the infringing instrumentalities include an interface hub application for integration. It uses SIP for nurse call systems and HL7 for EHR as well as other clinical systems. This includes event notification as well.

37. Defendant's publicly available information indicates that the infringing instrumentalities utilize peer-to-peer messaging between healthcare professionals, ancillary service providers, administrative staff, caregivers, or patients. All users are identified by their email address and the QS Software Systems cloud servers route the messages from one user to

another. Peer-to-peer messaging does not depend on a mobile number and uses a combination of Public and Private Keys to ensure that all messages remain encrypted while in transit or at rest.

38. Defendant's publicly available information indicates that the infringing instrumentalities support both collaborative group chats as well as broadcast group messages.

39. Defendant's publicly available information indicates that the infringing instrumentalities operate such that documents, spreadsheets, PDFs, images, video, and audio files can be sent and received securely.

40. Defendant's publicly available information indicates that the infringing instrumentalities provide web-based accounts for both individual and group accounts. Individuals can manage their personal profiles and passwords. Group administrators can manage users, create, and manage sub-groups (including access privileges), tailor the security settings, manage devices, review activity logs, and assign multiple administrators. Additionally, group administrators can remotely lock and wipe data from an end user's device in the event the device is lost or stolen.

41. Defendant's publicly available information indicates that the infringing instrumentalities allow a user to mask the caller ID for calls outbound from the QS Software Systems.

42. Defendant's publicly available information indicates that the infringing instrumentalities operate such that documents can be uploaded from a user's device gallery or by taking a picture of the document, which can then be annotated, signed, and sent to other QS Software Systems users or uploaded directly to QliqSTOR.

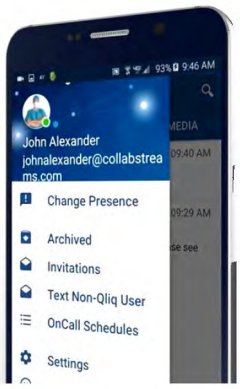
43. Defendant's publicly available information indicates that the infringing instrumentalities comprise secure texting that provides a user with the ability to remotely track the

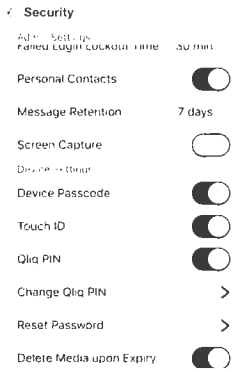
GPS locations of remote care teams. These functions enable group administrators to remote manage resources and direct them to the patients nearest to them.

44. Defendant's publicly available information indicates that the infringing instrumentalities provide active directory integration, giving users tools to sync credentials between QS Software Systems and other enterprise apps.

45. Defendant's publicly available information indicates that the infringing instrumentalities comprise archive features that receive a copy of all messages sent between users. All messages, attachments, and delivery status timestamps are stored.

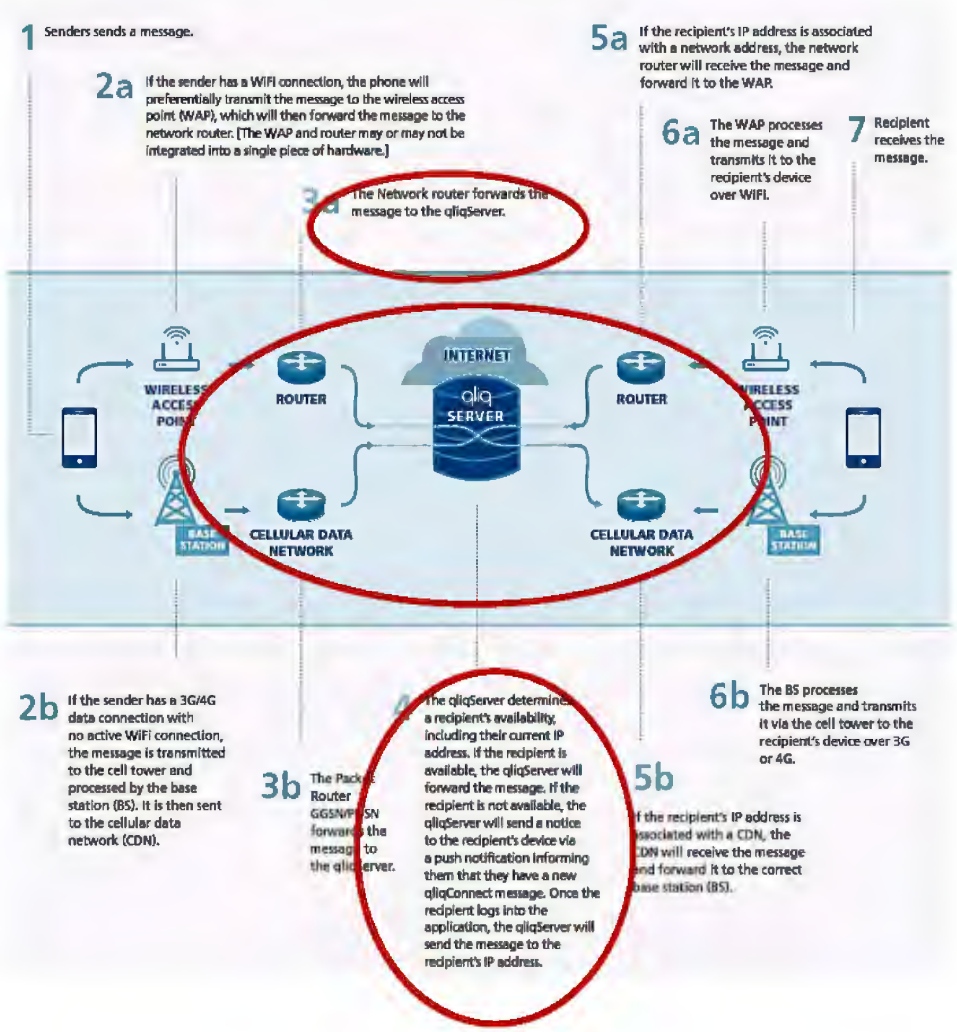
46. Defendant's publicly available information indicates that the infringing instrumentalities provides a display menu with user-selectable setting and options relevant to HIPAA compliance related parameters. For example, a user can select a message retention time:





47. Defendant's publicly available information indicates that the infringing instrumentalities operate such that messages are assigned lifespans so that they delete automatically, and administrators can remotely retract and delete any message that is sent or received on a mobile device that is subsequently lost, stolen, or otherwise disposed of:

48. Defendant's publicly available information indicates that the infringing instrumentalities operate such that the data flow of messages through those instrumentalities comprises routing message traffic through servers under the command, control, and operation of QliqSOFT:



49. Defendant's publicly available information indicates that the infringing instrumentalities monitor general activity on their servers and provide a detailed audit and logging report for users.

50. Defendant's publicly available information indicates that the infringing instrumentalities operate such that an administrator for a practice, group, or health system can back

up their data. The infringing instrumentalities enable a user to create a PDF and/or print conversations for inclusion in a patient's health record.

51. Defendant's publicly available information indicates that the infringing instrumentalities comprise secure messaging applications that assign a unique password and PIN code to each user so that they are the only ones who can decrypt the messages received.

52. Defendant's publicly available information indicates that the infringing instrumentalities' secure messaging applications are real-time and provide physicians access to data no matter where they are located.

53. Defendant's publicly available information indicates that the infringing instrumentalities operate such that a user may: navigate between secure texting, voice, and video calls; capture and share images, video, and audio; capture consent signatures; and/or communicate with external groups.

54. Defendant's publicly available information indicates that the infringing instrumentalities operate such that a user may: create, sign, and share PDFs; create and sign consents, referrals and more; upload images; and expedite workflow by uploading images and PDFs from the field into the EHR.

55. Defendant's publicly available information indicates that the infringing instrumentalities operate such that a user may tap an attachment icon to the left of the text field to reveal a media menu. A user can take a picture with the camera icon and record a video or audio clip to attach to a message.

56. Defendant's publicly available information indicates that the infringing instrumentalities provide the following features: customizable message notification and sound alerts; message delivery confirmation; manual message acknowledgement; custom lists of quick

messages; the ability to send images/videos/files/voice messages; organization of users by groups/subgroups; inclusion of external users; centralized administration; remote lock and wipe; message archiving; and EHR and directory integration.

57. Defendant's publicly available information indicates that the infringing instrumentalities operate such that messages exchanged contain metadata indicating the names of the users. Messages comprise metadata that get encrypted, or decrypted, respectively. Encryption is an indication of HIPAA compliance.

58. Defendant's publicly available information indicates that the infringing instrumentalities provide user search functions, to search subjects, messages, contacts, and groups. A user may also search contacts.

59. Defendant's publicly available information indicates that the infringing instrumentalities provide activity reports that display certain searchable user actions such as app login/logout, the time stamp details for each message, including who sent the message, the recipient, and when that message was created, sent, received, read, acknowledged, and deleted.

60. Defendant's publicly available information indicates that the infringing instrumentalities provide reporting tools that operate such that a user can enter a name or keyword in Search field to search across all message fields: sender, receiver, subject, and message. This searching can be further refined by sender, receiver, subject, message, and time range.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,426,730

61. Plaintiff herein restates and incorporates by reference paragraphs 16 – 60, above.

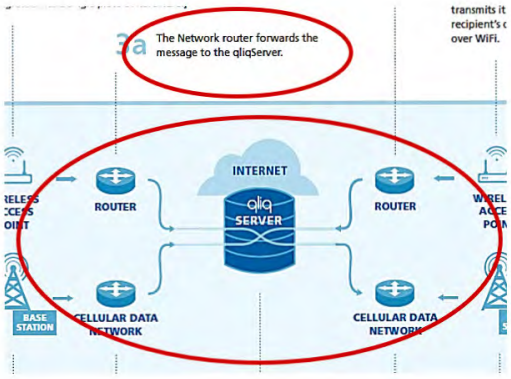
62. Plaintiff is the owner by assignment of United States Patent No. 7,426,730 ("the '730 Patent") entitled "Method and System for Generalized and Adaptive Transaction Processing Between Uniform Information Services and Applications" – including all rights to recover for past,

present, and future acts of infringement. The '730 Patent issued on September 16, 2008, and has a priority date of April 19, 2001. A true and correct copy of the '730 Patent is attached as Exhibit A, and hereafter incorporated by reference.

63. The '730 Patent discloses systems and methods providing a processing function that is useful for controlling any type of transaction between providers and consumers of information services. In particular, the invention provides a transaction framework that dynamically integrates a plurality of service providers and consumers based on transaction context data. (Ex. A, Col. 5, lines 12-17).

64. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for communicably coupling to, and providing access to, a plurality of networked data, communication, information, and application resources.

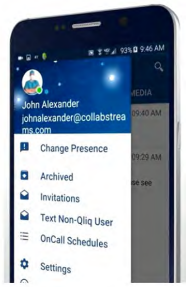
65. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities provide components that are communicably coupled to, and provide access to, a plurality of networked data, communication, information, and application resources ("Network Resources").

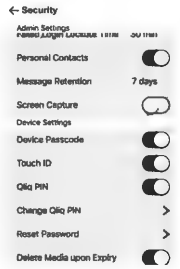


QliqCHAT Secure Texting provides a real-time, secure, HIPAA-compliant healthcare communication platform that connects every care team member and facilitates effective, patient-focused collaboration. We're securely bridging the communication and collaboration gap between doctors, nurses, patients, and even caregivers.

66. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for initiating a request from a client.

67. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities provide user interfaces, through which a user may initiate a request.

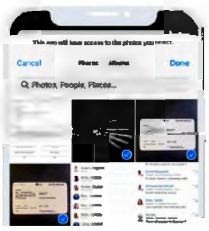




68. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for a resource information registry.

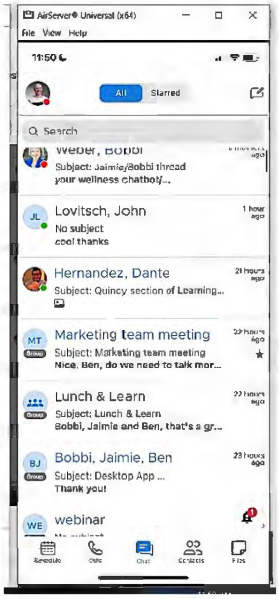
69. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities provide end users access to variety of Network Resources, listed and/or cataloged for the user (*e.g.*, via a directory).

To send media files you can tap the paperclip icon on the left side of the text field in a conversation. From here you can take a photo, access your media files as well as the QliqSTOR, EMR and Snap and Sign add ons if they have been enabled by your admin. From here you can select the media file you would like to share.



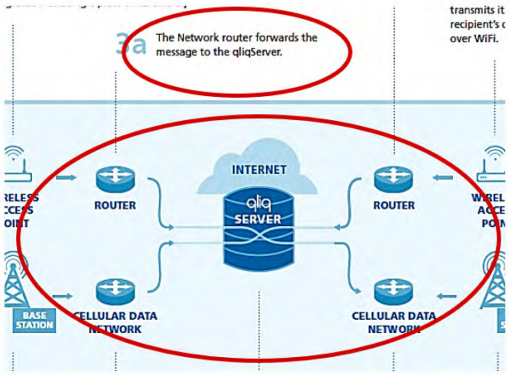
70. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for a user entering a transaction request defined or characterized by contextual elements.

71. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities, via a user interface, an end user enters a transaction request – defined or characterized by a number of contextual elements.



72. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for generating and processing transaction requests for access to Network Resources.

73. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities generate and process transaction requests for access to Network Resources.



QliqCHAT Secure Texting provides a real-time, secure, HIPAA-compliant healthcare communication platform that connects every care team member and facilitates effective, patient-focused collaboration. We're securely bridging the communication and collaboration gap between doctors, nurses, patients, and even caregivers.

74. Claims 1, 15, 17, 37, and 42 of the '730 Patent recite elements for processing a transaction request and delivering access to a responsive resource through a user interface.

75. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that the infringing instrumentalities process a transaction request, select one or more responsive resources, and deliver access to the responsive resource through a user interface.

76. Plaintiff herein restates and incorporates by reference paragraphs 16 – 75, above.

77. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that all recited elements of – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent are present on or within structure or operation of the Defendant's infringing instrumentalities.

78. As described in paragraphs 16 – 60, above, Defendant's publicly available information indicates that Defendant's infringing instrumentalities perform or comprise all required elements of – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent.

79. Defendant's infringing instrumentalities therefore literally infringe – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent.

80. In the alternative, the Defendant's infringing instrumentalities infringe – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent under the doctrine of equivalents. As described in paragraphs 16 – 60, above, Defendant's infringing instrumentalities perform substantially the same functions in substantially the same manner with substantially the same structures, obtaining substantially the same results, as the required elements of – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent. Any differences between the Defendant's infringing instrumentalities and the claims of the '730 Patent are insubstantial.

81. The Defendant's infringing instrumentalities, when used and/or operated in their intended manner or as designed, infringe – at least – claims 1, 15, 17, 37, and 42 of the '730 Patent, and Defendant is therefore liable for infringement of the '730 Patent.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Defendant has infringed the '730 Patent;

b. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith, from infringement of the '730 Patent;

c. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant's infringement of the '730 Patent as provided under 35 U.S.C. §§ 284, 286;

d. An award to Plaintiff for enhanced damages resulting from the knowing and deliberate nature of Defendant's prohibited conduct with notice being made at least as early as the service date of this complaint, as provided under 35 U.S.C. § 284;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

f. Any and all other relief to which Plaintiff may show itself to be entitled.

Respectfully Submitted,

By: */s/ K. Patrick Babb*
K. Patrick Babb
State Bar No. 24077060
E-mail: pbabb@foxrothschild.com
FOX ROTHSCHILD LLP
Saint Ann Court
2501 N. Harwood Street, Suite 1800
Dallas, Texas 75201
(972) 991-0889
(972) 404-0516 (Facsimile)
ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was served on counsel of record for Plaintiff in accordance with the Federal Rules of Civil Procedure on January 26, 2024.

/s/ K. Patrick Babb
K. Patrick Babb